Carnegie Mellon
Software Engineering Institute

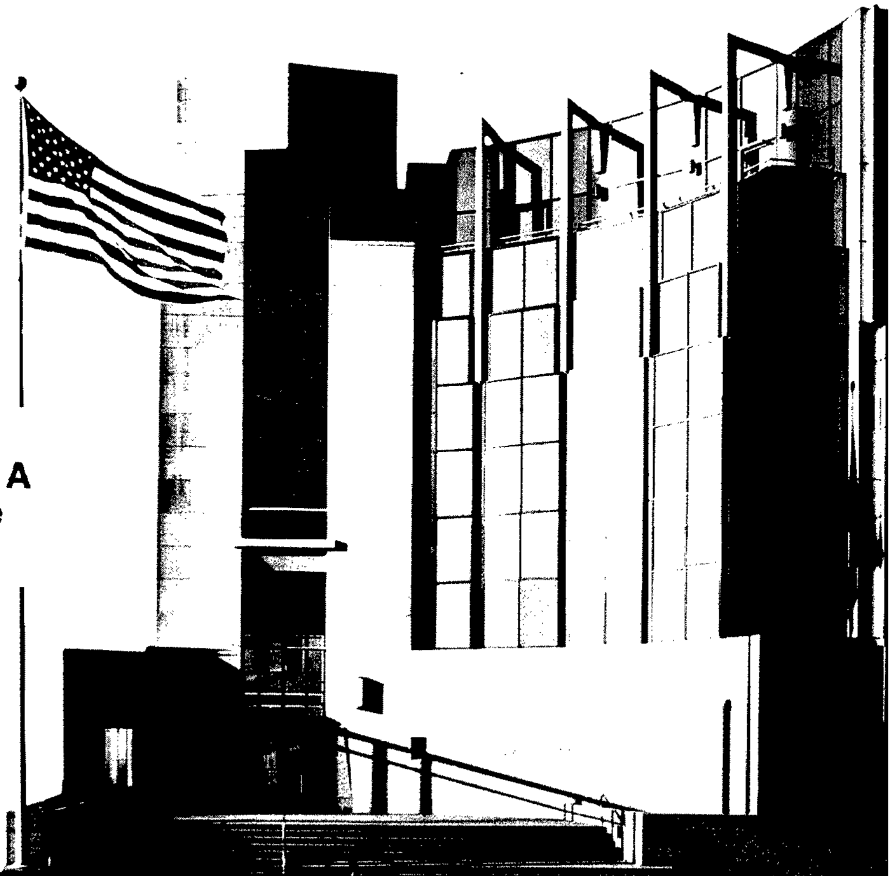
Promising Technologies for Future Systems

Grace A. Lewis
Edwin J. Morris
Lutz Wrage

December 2004

Integration of Software-Intensive Systems (ISIS)

Technical Note
CMU/SEI-2004-TN-043



Promising Technologies for Future Systems

Grace A. Lewis
Edwin J. Morris
Lutz Wrage

December 2004

Integration of Software-Intensive Systems (ISIS)

Technical Note
CMU/SEI-2004-TN-043

This work is sponsored by the U.S. Department of Defense.

The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this report is not intended in any way to infringe on the rights of the trademark holder.

This work was created in the performance of Federal Government Contract Number F19628-00-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

For information about purchasing paper copies of SEI reports, please visit the publications portion of our Web site (http://www.sei.cmu.edu/publications/pubweb.html).

Contents

List of Figures

List of Tables

Abstract

Joint Vision 2020, set forth by the Department of Defense, places a number of non-trivial, challenging requirements on future systems: data integration from distributed, dynamic, heterogeneous sources on the fly, and networks robust and fast enough to support secure real-time manipulation, fusion, and presentation of all this data. This technical note presents a few of the many programs, technologies, and research efforts that are addressing the challenges faced by future systems.

1 Introduction

Joint Vision 2020, set forth by the Department of Defense, states that future military operations will be increasingly conducted jointly, both with multiple branches of the U.S. Armed Forces and with allied and coalition forces, requiring increased levels of interoperability [ATO 04]. This vision places a number of non-trivial, challenging requirements on future systems.

- Future systems will require the capability to rapidly integrate data from distributed, heterogeneous, dynamic entities; present the relevant information in a form useful to command decision makers; formulate an integrated response; and bring the appropriate forces to bear.
- Future systems will require assembly on the fly, as dictated by evolving mission needs.
- A collaborative networking infrastructure that supports secure near-real-time manipulation and sharing of massive amounts of increasingly complex information, collected and fused from diverse sources, is required to facilitate ad-hoc teams.

This technical note presents of a few of the many programs, technologies, and research efforts that are addressing the challenges faced by future systems. Section 2 presents FORCEnet and Joint Battlespace Infosphere (JBI) as two Department of Defense (DoD) programs that are facing the challenges of Joint Vision 2020. Section 3 presents the Open Grid Services Architecture (OGSA) as a promising technology for building future systems. Section 4 presents the results of two projects sponsored by the Defense Advanced Research Projects Agency (DARPA), related to building secure systems on the fly.

2 DoD Programs

The vision being pursued by the U.S. Military to attain and exploit information superiority is known as net-centric warfare (NCW). NCW links sensors, communications systems, and weapons systems in an interconnected grid that allows for seamless information flow to warfighters, policy makers, and support personnel [DoD 01]. Many Department of Defense (DoD) programs are working on implementing capabilities to conduct NCW. FORCEnet and JBI are two examples of these programs [Morris 04].

2.1 FORCEnet

Net-centric operations and warfare (NCOW) is the DoD operational concept for NCW, linking platforms, computers, and people into a shared, state-of-the-art network (the Global Information Grid or GIG—see Section 3 for a short description) that integrates dispersed human decision makers, sensors, forces, and weapons into a highly adaptive, comprehensive system to achieve unprecedented mission effectiveness.

FORCEnet is both a U.S. Navy concept of how NCOW will be achieved and the Navy's implementation of their portion of the GIG It is intended to facilitate the integration of data, command and control, and combat capabilities at sea, on land, in the air, and in space. It is also intended to provide seamless integration and interoperation with joint, allied, and coalition forces [NNWC 04].

The FORCEnet engineering effort is not a traditional program in that it is not an acquisition effort and does not involve a prime contractor. Instead, it is an alignment effort directed at identifying the appropriate requirements, architectures, standards, and protocols by which the Navy can achieve the FORCEnet concept. In keeping with this strategy, the budget for FORCEnet engineering is small, gradually increasing from 15.7M to 23M from FY05 through FY09.

In order to achieve the FORCEnet (and NCOW) vision, the Navy will first focus on systemic network problems within the force, including

- insufficient bandwidth for high levels of information sharing
- multiple, poorly integrated networks and systems
- limited fusion of information from various manned and unmanned sources
- primitive information sharing with coalition partners based on workarounds

For the near- to mid-term future, FORCEnet engineering will focus on the infrastructure required to achieve the vision by specifying and architecting dynamic, survivable networks that provide increased and better managed bandwidth for the Navy's portion of the GIG The effort will also define information architectures that incorporate data from many sources, including unmanned sensors, making the resulting information available to tactical units.

Over the longer term, the FORCEnet engineering effort will develop the requirements, architectures, standards, and protocols to enable

- real-time common tactical pictures and visualization capabilities
- pervasive sensors across all spectrums (seabed to space)
- integrated and scalable mission planning with real-time modeling and simulation capability
- smart computer-based "agents" for organizing and managing information on the network
- hugely expanded bandwidth at sea
- seamless integration with parallel U.S. Army and U.S. Air Force capabilities
- support for new types of combat systems (e.g., energy-based weapons, wearable and undersea communications)

If this vision plays out, FORCEnet will ultimately become more than the Navy's GIG and transform into capabilities that directly support NCOW.

The FORCEnet organization is cognizant of the difficulties involved in reaching either the shorter or longer term goals. The organization must build consensus on requirements and architecture for the extremely complex and technically optimistic, but poorly understood vision. It must encourage managers (who control most acquisition dollars) to potentially act against the immediate interests of their programs and implement FORCEnet directives to employ unfamiliar technologies and approaches. While embracing the necessary new technologies, FORCEnet must be designed to interoperate with legacy systems, other military services, and coalition forces.

FORCEnet is relying on aggressive experimentation and prototyping to validate requirements, architectures, and technical and operational approaches. With only a small funding stream, it hopes to spark change by encouraging commercial contractors and Navy programs to voluntarily participate in FORCEnet planning and experimentation, and by providing a FORCEnet compliance checklist that ensures that programs are FORCEnet- and GIG- compliant.

2.2 Joint Battlespace Infosphere (JBI)

A major problem that must be overcome to achieve the NCOW vision is the limited integration between the major DoD combat information systems. Information within these systems is disjointed, inconsistent, often overlapping, and defined and formatted in ways that are incomprehensible to other systems. As a result, there is no common operational picture.

The Joint Battlespace Infosphere[1] (JBI) Research and Development (R&D) program directed by Air Force Research Laboratory Information Directorate is addressing this problem by defining a common information management environment that integrates data from many sources. JBI will also manipulate that data to create actionable information and make it available at the appropriate level to users [AFRL 03].

JBI is intended to both integrate data from the many stovepiped information systems that currently support the forces, and to provide an architecture for future sensors, tools, and planning aides. JBI will act as an intermediary between systems, converting information into appropriate formats and fusing information to create a more complete situational picture.

The thrust of the JBI program is to develop core services that

- control access to information (e.g., authentication, authorization)
- allow clients to publish, subscribe, and query
- manipulate and enhance the value of information through techniques such as filtering and aggregation via *fuselets.* A fuselet is a special kind of client that can refine or fuse information from one or more sources to create information in a form required by users [Milligan 04].
- facilitate the integration of organizations into the "infosphere" by describing organizational information needs, products, and capabilities via *force templates.* Force templates identify entities to (primarily) correspond to military units and support organizations [Marmelstein 02].

A key problem for JBI is the definition of an appropriate strategy and technologies that allow the sharing of the semantic information that is embedded deep within the data and processing of applications. JBI is investigating a range of technologies to address this problem. Several promising technologies are discussed in the following paragraphs.

A combination of available technologies such as eXtensible Markup Language (XML), Resource Description Framework (RDF), and RDF Schema allow computer sharing of metadata that defines the type, structure, location and other information about resources on a Web. These technologies (particularly XML) are becoming a common foundation for Web information sharing. However, the technologies alone are not sufficient for sharing of semantic information, or for answering critical questions such as how a particular concept in one system (e.g., a "track") is related to concepts in other systems.

The Web Ontology Language (OWL) builds on RDF and RDF Schema and adds vocabulary for describing properties (e.g., symmetric, inverse of), classes (e.g., definition, subclass, equivalence), and relationships (e.g., cardinality) [W3C 04]. OWL can be used to represent ontologies—domain vocabularies that define the precise meanings of specific terms and relationships between those terms. Unfortunately, OWL is immature, and presumes the ability to develop shared ontologies. Building a shared ontology for the complex information

[1] *Infosphere* means "the sum of all information available."

contained in hundreds of independently developed legacy and new Air Force systems is a daunting prospect.

Even if appropriate ontologies can be built, additional questions remain regarding how to share information about how a service works and regarding the qualities of service (e.g., accuracy, reliability) provided. OWL-S is an extension of OWL and other technologies that provides a means for sharing information about service invocation, enactment, composition, monitoring, and recovery. In addition, OWL-S provides a mechanism for specifying the non-functional properties of a service, such as security requirements and quality of service [Martin 04]. A beta version of OWL-S that can serve as a basis for research and discussion of semantic Web Services was released in mid-2004.

Beyond trying to find solutions to the key problem of conveying semantic content, JBI has identified the need to create a fuselet. As we've noted, a fuselet is a special kind of client that can refine or fuse information from one or more sources to create information in a form required by users [Milligan 04]. Fuselets are intended for purposes such as transforming information formats from one system into formats required by another system, and combining information from multiple systems to supply a fused operational picture. Fuselets will get their information from the JBI information space by subscribing to or querying information objects, execute appropriate decision logic, and create new information objects.

In order to support "composable" combat forces and the anticipated fluid nature of military activities, there must also be ways for military assets to efficiently "plug in" to JBI and identify the capabilities and data the asset provides and requires. In order to provide this capability, JBI has defined a force template. We've noted that a force template identifies entities to (primarily) correspond to military units and support organizations [Marmelstein 02]. Entities are composed of other entities (e.g., smaller organizations or units) and clients (e.g., specific systems, platforms, individuals). The infospheres that can be built up with clients and entities (and the associated force templates) reflect the manner in which U.S. and (potentially) coalition forces could be combined to achieve an operational goal. In addition to providing information about what organizations can provide and require, the force template can provide other critical information including

- quality of service
- time frame for service delivery
- security expectations
- accuracy of information
- ontologies
- fuselets

JBI can potentially serve as a gateway tying together the capabilities of the future U.S. Navy FORCEnet with parallel U.S. Air Force C2 Constellation and U.S. Army Future Combat Systems capabilities. In addition, JBI may serve to tie in other government (e.g., Homeland Security) and non-government agencies, as well as the capabilities of coalition allies.

Related Programs

C2 Constellation

The C2 Constellation is an Air Force program established in 2000, designed to support NCW and JV2020. The goal of this program is stated as

C2 Constellation will facilitate the development of decisive information superiority, collaborative planning, and synchronized operations for the warfighters by promoting interoperability and integration between systems that support Command, Control, Computing, Communication, Intelligence, Surveillance, and Reconnaissance (C4ISR). The C2 Constellation promotes rapid access to data stores that support situational awareness, effects based operations, and predictive battlespace awareness [Sweet 04].

C2 Constellation plans to use Service-Oriented Architectures (SOA) and Web Services as technologies to reach its objective.

Future Combat Systems (FCS)

FCS is a joint program that will develop net-centric concepts in support of the U.S. Army's goal to be fully transformed and attain "Future Force" (formerly "Objective Force") by the end of this decade. FCS is a networked "system of systems"—one large system made up of 18 individual systems, plus the network, plus the soldier. It utilizes advanced communications and technologies to link soldiers with both manned and unmanned ground and air platforms and sensors [Boeing 04].

The Lead Systems Integrator (LSI) completed the initial Concept and Technology Development (CTD) phase and transitioned to the System Development and Demonstration (SDD) phase in 2003. The goal for FCS is to have the first unit equipped in 2008 and an initial operational capability (IOC) in 2010.

3 Technologies

The majority of today's military systems are stove-piped and static—they are conceived, designed, constructed, and maintained to address a particular need or problem. However, future military capabilities must be scalable and dynamic to meet a range of conflict types and expectations placed on the military. One promising technology for developing and assembling highly dynamic military capabilities that can be tailored to specific situations is the Open Grid Services Architecture (OGSA).

3.1 Open Grid Services Architecture (OGSA)

Grid computing is a form of distributed computing that involves coordinating and sharing computing, application, data, storage, or network resources across dynamic and geographically dispersed organizations [Grid 04].

The Open Grid Services Architecture (OGSA) is a non-proprietary effort by Argonne National Laboratory, IBM, the University of Chicago and other institutions, that combines grid computing with Web services. The goal of this architecture is to enable the integration of geographically and organizationally distributed components to form virtual computing systems that are sufficiently integrated to deliver desired Quality of Service (QoS).

OGSA defines the mechanisms for creating, managing, and exchanging information among entities, called *Grid Services*. The Open Grid Services Infrastructure (OGSI) defines the standard interfaces and behaviors of a Grid Service [GGF 03]. The Globus Toolkit is an open source implementation of Version 1 of the OGSI Specification. Release 3.2 is available for download from the Globus Alliance Web site [Globus 04, Sandholm 03].

As stated previously, OGSA represents everything as a Grid Service. Grid Services are stateful transient Web service instances that are discovered and created dynamically to form larger systems [Foster 02a]. Transience has significant implications for how services are managed, named, discovered, and used—and transience is what makes a Grid Service different from a Web Service. A Grid Service conforms to a set of conventions, expressed as WSDL interfaces, extensions, and behaviors, for such purposes as

- discovery—mechanisms for discovering available services and for determining the characteristics of those services so that they can be invoked appropriately
- dynamic service creation—mechanisms for dynamically creating and managing new service instances

- lifetime management—mechanisms for reclaiming services and state in the case of failed operations
- notification—mechanisms for asynchronously notifying changes in state

As OGSA evolves it will include interfaces for authorization, policy management, concurrency control, and monitoring and management of potentially large sets of Grid Service instances.

The current release of the Globus Toolkit, as presented in Figure 1, contains the following interface definitions:

- OGSI Reference Implementation—implementations for all OGSI specified interfaces
- Security Infrastructure Implementation—SOAP as well as transport level message protection, end-to-end mutual authentication, and single sign-on service authorization
- System-Level Services—infrastructure level run-time services
- Base Services—higher-level services such as Program Execution, Data Management, and Information Services.

The intention of these interface definitions is to provide building blocks that can be reused to implement a variety of higher-level Grid Services, such as distributed data management services, workflow services, auditing services, instrumentation and monitoring services, problem determination services, and security protocol mapping services. Users can also define their own higher-level services.

All these services and primitives interact with the Grid Service Container—an abstract OGSI run-time environment. Finally, the Web Service Engine and Grid Service Container are hosted in a Hosting Environment, which implements traditional Web Server functionality [Sandholm 03].

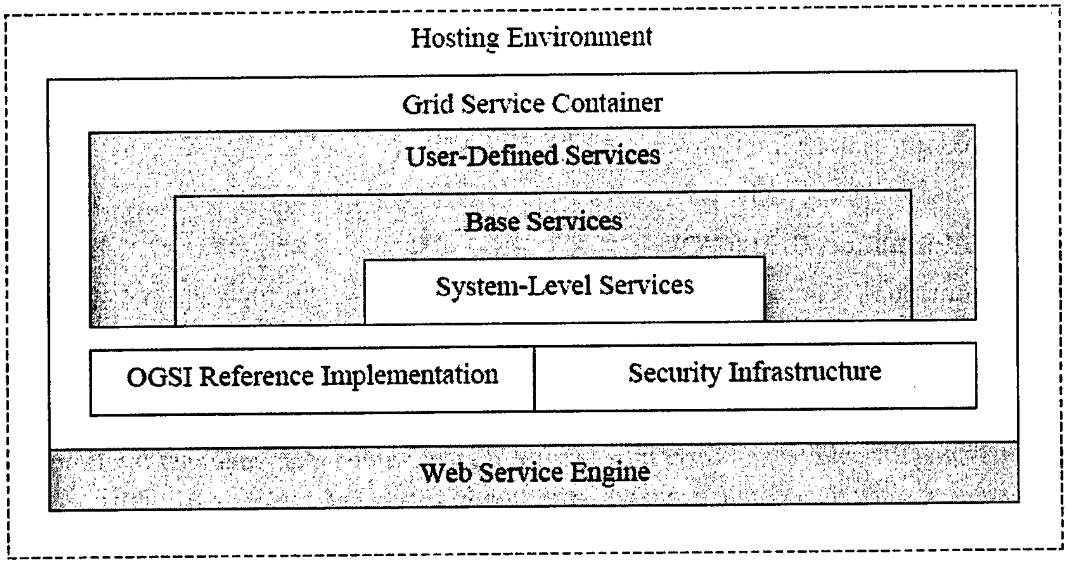


Figure 1: Globus Toolkit Architecture

This emerging technology is currently being used mainly in e-science and e-business applications. However, there is great potential for its use in mission-critical systems, such as in enabling collaborative targeting between multiple users and multiple sites. FORCEnet, for example, will depend upon a distributed computing environment to support gridded sensors, shooters, and decision makers. There is increasing support and research based on OGSA:

- extension of WSDL and UDDI to include QoS properties necessary for OGSA's objectives [Al-Ali 02, Sheth 02]
- OGSA interfaces for e-utilities—Web hosting, content distribution, applications, and storage service providers who offer continuous, on-demand access [Foster 02b]
- Hewlett Packard's Adaptive Enterprise strategy—synchronization between business and information technology (IT) [HP 03]
- ICENI – Imperial College e-Science Networked Infrastructure—service-oriented Grid middleware to support e-science [Furmento 02]
- Oracle 10g—Oracle supports OGSA and is integrating it into its 10g products
- IBM e-server and IBM total storage—two of the IBM products that support OGSA
- NSF Middleware Initiative (NMI)—distributes a pre-built Globus Toolkit with other relevant components [NMI 04]
- the North Carolina BioGrid Project— established to research and implement new Grid computing technologies that will enable researchers and educators throughout North Carolina to take full advantage of the genomic revolution [NC 04]

Given its growing industry support and the validity of its conceptual foundation, there is a good possibility that OGSA is a technology that will emerge as a standard for Grid computing.

Related Efforts

There are many DoD efforts that are related to Grid computing, including several already mentioned (e.g., FORCEnet, C2 Constellation). At the core of these efforts is the desire to establish a Global Information Grid infrastructure to support NCOW. A brief discussion of the Global Information Grid follows.

Global Information Grid (GIG)

In a memorandum, "Global Information Grid," dated September 22, 1999, the DoD CIO issued guidance on the definition and scope of the GIG It defined the GIG as

a globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel.

In short, the GIG is directed towards providing critical networking infrastructure to the forces, essential for achieving NCW. The concepts and capabilities present in the GIG will be the means to achieve what is called *information superiority*—a relative information advantage vis-à-vis an adversary.

Both OGSA and the GIG are based on Grid computing, but they work at different levels. The GIG works more at the infrastructure level, while OGSA works more at the middleware level. That is, OGSA assumes an underlying infrastructure, while the GIG is an infrastructure in itself with a number of added services, as illustrated in Figure 2 [DoD 01].

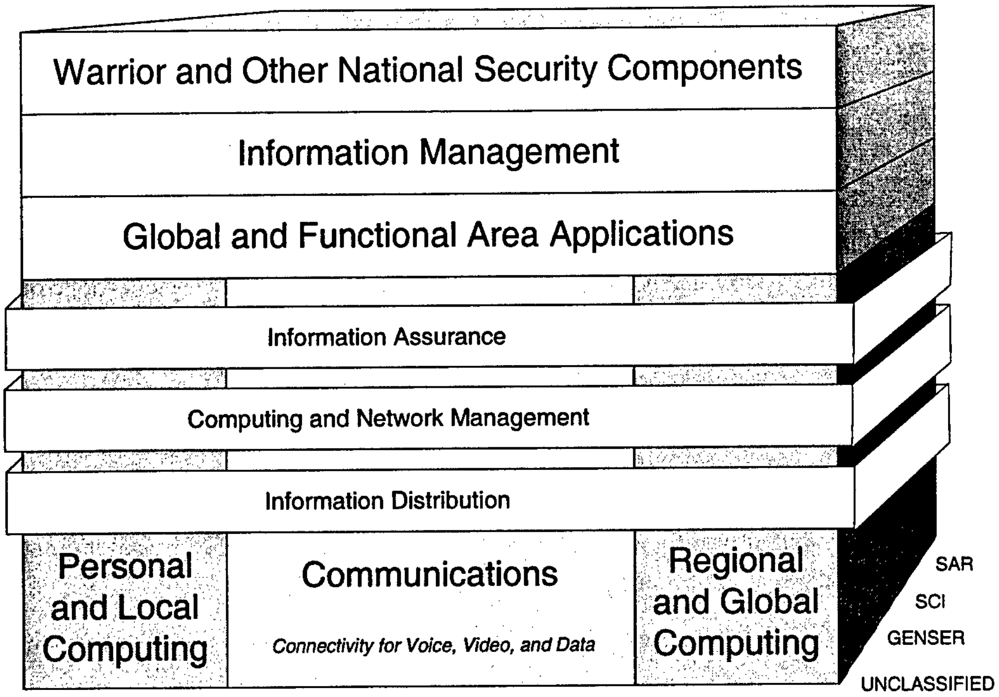

Warrior and Other National Security Components
Information Management
Global and Functional Area Applications
Information Assurance
Computing and Network Management
Information Distribution
Personal and Local Computing
Communications
Connectivity for Voice, Video, and Data
Regional and Global Computing
SAR
SCI
GENSER
UNCLASSIFIED

Figure 2: GIG Reference Model

There is great potential for collaboration between OGSA and the organizations in charge of implementing the GIG For example, in a memorandum, "GIG Information Management" dated August 24, 2000, there is guidance for "… discovery, retrieval, and management of the flow of GIG information; implementation of mechanisms for access and delivery; processes and methods to facilitate the proper understanding and use of information …" These could be implemented as OGSA higher-level services. Another possibility is for the Globus Toolkit to provide bindings so that OGSA Grid Services can be built on top of the GIG There was an interesting DARPA proposal to investigate the on-demand creation of systems through the combination of core services and dynamically recruited services. These services would be built on top of OGSA [NICCI 02]. This proposal was unfortunately not funded.

4 Research Projects

Many research projects are focusing on dynamically-built secure systems—one of the many challenges for future systems. We will look at two DARPA-sponsored projects, Control of Agent Based Systems (CoABS) and Integrated Security Services for Dynamic Coalition Management.

4.1 Control of Agent Based Systems (CoABS)

CoABS is a program that was funded by DARPA from 1999 until 2003. Overall it comprised 20+ research and demonstration projects.

The goal of the program was to develop and demonstrate techniques to safely control, coordinate, and manage large systems of autonomous software agents. CoABS investigated the use of agent technology to improve military command, control, communication, and intelligence gathering based on the need to "rapidly assemble a set of disparate information systems into a coherently interoperating whole" [Schmorrow 02].

Software agents are components that are capable of acting autonomously in order to accomplish tasks on behalf of their users. The following characteristics of software agents are of interest in the context of the CoABS program:

- mobile code—processing moves to information sources so there is no need to transfer all data over limited/bursty bandwidth connections
- "disembodied" code with temporal duration or persistent state—software agents work autonomously when not connected to their users
- semantic broker and namespace services—services and information are located by semantic content; agents mediate interoperability
- dynamic services and control protocols—access to an adaptive community of disconnected and dynamically-changing heterogeneous resources

The CoABS program comprised three major tasks areas [Schmorrow 02].

1. Agent Grid—a task focused on the development of tools that form a basis for upgrading military legacy systems to take advantage of agent technology. The Agent Grid is a middleware-based approach, where agents connect to the Grid through

"Grid connectors." Grid connectors can wrap legacy systems to enable those systems to provide services to other systems connected to the Grid.

2. Agent Interoperability Standards—a task to define standards that support interaction between agent and human, communication between agents, software interfaces for agents, and agent management and control. Standards are regarded as the most effective way to improve interoperability.

3. Scaling of Agent Control Strategies—the Agent Grid must be able to support a large number of interacting agents. This task focuses on monitoring, coordination, control, and management of agent collections. These strategies must be able to enforce guaranteed behaviors even if the underlying network is unreliable.

Some of the results of the CoABS program are highlighted in [DARPA 03]. The program

- released CoABS Grid code and components tailored to military user needs
- demonstrated the scalability of the architecture to support more than 1,000 agents without conflicts
- demonstrated and evaluated CoABS in military applications including major joint exercises featuring coalition operations
- demonstrated the capability of the CoABS technology to support a heterogeneous network of platforms and weapons systems to provide an order of magnitude improvement in naval combat flexibility and operational effectiveness

CoABS is no longer an active DARPA program, but there are many programs that use or have used concepts or technology developed in the CoABS program. The following table summarizes these programs.

Table 1: CoABS Transition

Program	**Organization**
Expeditionary Sensor Grid	Navy Warfare Development Command
Coalition Agents Experiment (CoAX) outreach to Coalition Partner	DARPA CoABS, Australia (DSTO), the UK (DSTL) and the U.S. (AFRL/Rome)
Airborne Manned/Unmanned System Technology (AMUST) Program	Army Aviation Applied Technology Directorate (AATD)

Integrated Flight Management/Advanced Technology Demonstration (IDM/ATD)	Information Directorate of the Air Force Research Lab (AFRL/IF)
Effect Based Operations (EBO)	Information Directorate of the Air Force Research Lab (AFRL/IF)
Joint Battlespace Infosphere	Information Directorate of the Air Force Research Lab (AFRL/IF)

In addition to the above mentioned programs the DARPA is funding the Collaborative Cognition program which builds on CoABS.

4.2 Integrated Security Services for Dynamic Coalition Management

Integrated Security Services for Dynamic Coalition Management is a DARPA-sponsored project managed by U.S. Air Force Research Laboratory that started in March 2000 with a duration of 36 months. The work was performed at the University of Maryland.

Coalitions are collaborative networks of autonomous domains where resource sharing is achieved by the distribution of access permissions to coalition members based on negotiated resource-sharing agreements—common access states. A dynamic coalition is formed when members may leave or new domains may join during the life of the coalition. To support security in dynamic coalitions, this project had two goals: (1) to enable the creation and management of coalitions with diverse and rapidly changing membership, and (2) to provide solutions to fundamental problems of integrating diverse access control policies, public key infrastructure (PKI), and group communication technologies for dynamic coalition [Khurana 03].

The project developed a prototype of tools for coalition infrastructure services, which includes joint policy administration services, certificate services, and group communication services. The tools support the joining, voluntary departure, and involuntary departure of coalition members. Accomplishments that are important to future systems include

- definition of a common language to express access control policies using a Role-Based Access Control (RBAC) policy model
- automatic computation of access control states using constraint language and computation
- dynamic adaptation of policies based on joining and exit of participants

The results of this work are critically important to support the dynamic coalitions' sharing of classified and unclassified information envisioned for NCW.

Related Efforts

Dynamic Coalitions

The Advanced Technology Office (ATO) in DARPA is the sponsor for the Dynamic Coalitions program. Its mission is to develop technologies to support the secure creation of dynamic coalitions, including the necessary technologies for policy management, group communications, supporting security infrastructure services, data sharing, and joint collaboration spaces. The work outlined by this program is mainly in the area of security, but goes beyond the scope of the work outlined in the Integrated Security Services for Dynamic Coalitions just described. Among other projects, it plans to investigate wireless networking technologies to move security to the interface, develop cryptographic hardware accelerators to speed up cryptographic computations, and develop a modular architecture and robust key agreement within a dynamic coalition [ATO 04].

Information On-Demand

At a recent DARPA conference, program managers from DARPA's ATO outlined the need for dynamic security and reliability to accompany the presence of a network; this is why it is funding so many projects in this area [French 04a]. For example, DARPA recently awarded a contract to Computer Systems Center Inc. (CSCI) for work on dynamic network security applications. The project is called Information-on-Demand and is basically a study to determine whether dynamic network security access is possible [French 04b].

The basis for CSCI's work will be its product—Trusted Information Infrastructure (TII). TII is designed to allow the secure transfer of information between secure networks at multiple levels [CSCI 04].

5 Conclusions

This technical note discusses a small sample of promising work aimed at meeting the challenges of future military systems. Meeting the challenges for future systems will not be easy. To assemble systems on the fly, integrate data from distributed, heterogeneous and dynamic sources, and support dynamic organization of combat capabilities is going to require advances in networking, semantic description of data, and mechanisms to convey the quality of service attributes (e.g., security, reliability, accuracy) of the entities providing the data.

Meeting these challenges will entail greater funding for basic research, as well as realistic levels of expectations and support for military programs attempting to employ the fruits of that research. Both are critical. The basic research should continue to develop and mature mechanisms to assemble systems and convey meaning among them, while programs such as FORCEnet will help clarify poorly understood requirements for dynamic, grid-oriented systems, as well as verify the value of the technologies under development. If research can be aligned with the programs and policies intended to promote and incentivize joint operations, Joint Vision 2020 has a much greater chance of becoming reality.

References

URLs are valid as of the publication date of this document.

[AFRL 03] Air Force Research Laboratory. *Joint Battlespace Infosphere (JBI).* Rome Laboratory, N.Y: Air Force Research Laboratory, 2003. http://www.rl.af.mil/programs/jbi/

[Al-Ali 02] Al-Ali, R.; Rana, O.; Walker, D.; Jha, S. & Sohail, S. "G-QoSM: Grid Service Discovery Using QoS Properties." *Computing and Informatics Journal, 21*, 4 (2002): 363-82.

[ATO 04] Advanced Technology Office (ATO). *Dynamic Coalitions Program* Arlington, VA: Defense Advanced Research Projects Agency (DARPA). http://www.darpa.mil/ato/programs/dynamiccoal.htm

[Boeing 04] Boeing. *Future Combat Systems*. Chicago, IL: Boeing World Headquarters, 2003. http://www.boeing.com/defense-space/ic/fcs/bia/flash.html

[CSCI 04] CSCI. *Trusted Information Infrastructure (TII).* Springfield, VA: CSCI (Computer Systems Center Incorporated) Headquarters, 2004. http://www.csci-va.com/csciweb/csciwebsite.nsf

[DARPA 03] DARPA. "Fiscal Year (FY) 2004/FY 2005 Biennial Budget Estimates," February 2003. *Research, Development, Test and Evaluation, Defense-Wide: Volume 1 - Defense Advanced Research Projects Agency*. Washington, DC: United States Department of Defense, 2003. http://ec.sei.cmu.edu/keywords/new.htm. http://www.darpa.mil/body/pdf /FY04_FY05BiennialBudgetEstimatesFeb03.pdf

[DoD 01] Department of Defense. *Network Centric Warfare: Report to Congress.* Washington, DC: United States Department of Defense, 2001. http://www.defenselink.mil/nii/NCW/ncw_main.pdf

[Foster 02a] Foster, I.; Kesselman, C.; Nick, J. & Tuecke, S. "The Physiology of the Grid: An Open Grid Services Architecture for Distributed Systems Integration." *Open Grid Service Infrastructure WG, Global*

Grid Forum, Lemont, IL, June 22, 2002. http://www.gridforum.org /ogsi-wg/drafts/ogsa_draft2.9_2002-06-22.pdf

[Foster 02b] Foster, I.; Kesselman, C.; Nick, J. & Tuecke, S. "Grid Services for Distributed System Integration." *IEEE Computer 35*, 6 (June 2002): 37-46. http://www.globus.org/research/papers/ieee-cs-2.pdf

[French 04a] French, M. "Net-centric War Needs Security." *Federal Computer Week (FCW.com),* March 11, 2004. http://www.fcw.com/fcw /articles/2004/0308/web-darpa-03-11-04.asp

[French 04b] French M. "DARPA awards network security deal." *Federal Computer Week (FCW.com),* February 23, 2004. http://www.fcw.com/fcw/articles/2004/0223 /web-darpa-02-23-04.asp

[Furmento 02] Furmento, N.; Mayer, A.; McGough, S.; Newhouse, S.; Field, T.; & Darlington, J. "ICENI: Optimization of Component Applications Within a Grid Environment." *Parallel Computing* 28, *12* (Dec. 2002): 1753-1772.

[GGF 03] Global Grid Forum—Open Grid Services Infrastructure Working Group. *Open Grid Services Infrastructure (OGSI) Version 1.0.* June 2003.Lemont, IL, Global Grid Forum, 2003. http://www-unix.globus.org/toolkit /draft-ggf-ogsi-gridservice-33_2003-06-27.pdf.

[Globus 04] The Globus Alliance. Chicago, IL: University of Chicago, 2004. http://www.globus.org/ogsa/

[Grid 04] Grid.org. Austin, TX: United Devices, Inc., 2004. http://www.grid.org.

[HP 03] Hewlett-Packard. News Release: "HP Advances Grid Strategy for the Adaptive Enterprise." Palo Alto, CA: Hewlett-Packard, 2003. http://www.hp.com/hpinfo/newsroom/press/2003/030904b.html

[Khurana 03] Khurana, H.; Gavrila, S; Bobba, R.; Koleva, R.; Sonalker A.; Dinu, E.; Gligor, V. & Baras, J. "Integrated Security Services for Dynamic Coalitions." *Proceedings of the DARPA Information Survivability Conference and Exposition.* April 22-24, 2003, Washington, DC. Los Alamitos, CA: IEEE Computer Society, 2003.

[Marmelstein 02] Marmelstein, R. “Force Templates: A Blueprint for Coalition Interaction within an Infosphere.” *IEEE Intelligent Systems 17*, 3, (May-June 2002): 36-41.

[Martin 04] Martin, D.; Paolucci, M.; McIlraith, S.; Burstein, M.; McDermott, D.; McGuinness, D.; Parsia, B.; Payne, T.; Sabou, M.; Solanki, M.; Srinivasan, N.; and Sycara, K. “Bringing Semantics to Web Services: The OWL-S Approach” *Proceedings of the First International Workshop on Semantic Web Services and Web Process Composition (SWSWPC 2004),* 2004 IEEE International Conference on Web Services (ICWS'2004) July 6-9, 2004, San Diego, CA. Los Alamitos, CA: IEEE Computer Society, 2004.

[Milligan 04] Milligan, J. *Draft Concept of Operation for Joint Battlespace Infosphere (JBI) Fuselets.* AFRL/IFSE Joint Battlespace Infosphere (JBI) Air Force Research Laboratory Information Directorate, 23 June 2004. http://www.fuselet.org/specifications /FuseletCONOPS-V1.1-23Jun04.doc

[Morris 04] Morris, E.; Levine, L.; Meyers, C.; Place, P.; & Plakosh, D. *Systems of Systems Interoperability.* (CMU/SEI-2004-TR-004). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2004. http://www.sei.cmu.edu/publications /documents/04.reports /04tr004.html

[NC 04] *North Carolina BioGrid Project.* Research Triangle Park, NC: MCNC Corporation, 2004. http://www.ncbiogrid.org/

[NICCI 02] *Network-Centric Infrastructure for Command, Control and Intelligence.* Presolicitation Experimentation Plan. Arlington, VA: Defense Advanced Research Projects Agency (DARPA), Nov. 2002. http://ec.sei.cmu.edu/keywords/new.htm.

[NMI 04] *NSF Middleware Initiative.* Arlington, VA: National Science Foundation Middleware Initiative, 2004. http://www.nsf-middleware.org/

[NNWC 04] *Naval Network Warfare Command.* FORCEnet. Norfolk, VA: FORCEnet Content Manager, 2004. http://forcenet.navy.mil/

[Sandholm 03] Sandholm, T. & Gawor, J. *Globus Toolkit 3 Core – A Grid Service Container Framework.* Chicago, IL: Globus Toolkit Core White Paper, 2003.

http://www-unix.globus.org/toolkit/3.0/ogsa/docs /gt3_core.pdf

[Salasin 03] Salasin J. & Moini A. "Leveraging Grid Technology in Network-centric Environments." *Proceedings of the Second IEEE International Symposium on Network Computing and Applications (NCA'03).* April 16-18, 2003. Cambridge, MA. Los Alamitos, CA: IEEE Computer Society, 2003.

[Schmorrow 02] Schmorrow, D. "The DARPA Control of Agent Based Systems (CoABS) Program and Challenges for Collaborative Coalitions," 182-183. *Proceedings of the Second International Conference on Knowledge Systems for Coalition Operations (KSCO 02).* Toulouse, France, April 23-24, 2002. Springfield,VA: National Technical Information Service (NTIS), 2002.

[Sheth 02] Sheth, A.; Cardoso, J.; Miller, J.; Kochut, K.; & Kang, M. "QoS for Service-oriented Middleware," 528-34. *Proceedings of 6th World Multiconference on Systemics, Cybernetics and Informatics,* July 14-18, 2002, Orlando, FL. Orlando, FL: International Institute of Informatics and Systemics, 2002. http://lsdis.cs.uga.edu/lib/download/SCM+02-SCI2002.pdf

[Sweet 04] Sweet, N. & Kanefsky, S. "The C2 Constellation: A U.S. Air Force Network Centric Warfare Program - Network Centric Applications and C4ISR Architecture." *Technology Symposium: The Power of Information Age Concepts and Technologies.* June 15-17, 2004, San Diego, CA. Vienna, VA: Evidence Based Research, Inc., 2004. http://www.dodccrp.org/events/2004/CCRTS_San_Diego/CD/papers/164.pdf

[W3C 04] W3C. OWL *Web Ontology Language Guide.* Cambridge, MA: Massachusetts Institute of Technology, World Wide Web Consortium, 2004: http://www.w3.org/TR/owl-guide/

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY
(Leave Blank)

2. REPORT DATE
December 2004

3. REPORT TYPE AND DATES COVERED
Final

4. TITLE AND SUBTITLE
Promising Technologies for Future Systems

5. FUNDING NUMBERS
F19628-00-C-0003

6. AUTHOR(S)
Grace A. Lewis, Edwin J. Morris, Lutz Wrage

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

8. PERFORMING ORGANIZATION REPORT NUMBER
CMU/SEI-2004-TN-043

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
HQ ESC/XPK
5 Eglin Street
Hanscom AFB, MA 01731-2116

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified/Unlimited, DTIC, NTIS

12B DISTRIBUTION CODE

13. ABSTRACT (MAXIMUM 200 WORDS)

Joint Vision 2020, set forth by the Department of Defense, places a number of non-trivial, challenging requirements on future systems: data integration from distributed, dynamic, heterogeneous sources on the fly, and networks robust and fast enough to support secure real-time manipulation, fusion, and presentation of all this data. This technical note presents a few of the many programs, technologies, and research efforts that are addressing the challenges faced by future systems.

14. SUBJECT TERMS
Interoperability, FORCEnet, Joint Battlespace Infosphere, JBI,Open Grid Services Architecture, OGSA, Control Agent Based Systems, CoABS, Integrated Security Services for Dynamic Coalition Management

15. NUMBER OF PAGES
28

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT
Unclassified

18. SECURITY CLASSIFICATION OF THIS PAGE
Unclassified

19. SECURITY CLASSIFICATION OF ABSTRACT
Unclassified

20. LIMITATION OF ABSTRACT
UL